80 Eye-Opening Cyber Security Statistics for 2019 - Hashed Out by The SSL Store™

Cyber attacks have never been more prevalent than they will be in 2019

It's an interesting and challenging time to be working in the cyber security industry. By and large, research indicates that cybercrime is on the rise < https://www.thesslstore.com/blog/cybercrime-pays-new-study-finds-cybercriminal-revenues-hit-1-5-trillion-annually/> — news headlines support these findings as major companies like Marriott < https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/> , Equifax < https://www.thesslstore.com/blog/equifax-data-breach-total-data-lost-the-final-count/> , Yahoo < https://www.thesslstore.com/blog/yahoo-breach/> , and

Facebook < https://www.thesslstore.com/blog/facebook-network-breach/> find themselves in the crosshairs of cyber attacks. Even sacrosanct governmental election processes < https://www.pewglobal.org/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/> the world over are not excluded from falling prey to cybercriminals and are a part of the increasing statistics about cyber security and cyber attacks.

In this article, we’ll present you with essential cyber security statistics but also want to take a moment to recognize that this incredibly broad category encompasses many areas of concern for individuals, IT security professionals, and business leaders alike. This range of topics include everything from cyber security vulnerabilities such as unpatched software and expired security certificates < https://www.thesslstore.com/blog/what-happens-when-your-ssl-certificate-expires/> to the costs of cyber security attacks to the number of businesses that implement adequate (or inadequate <

https://www.thesslstore.com/blog/93-websites-fail-mozilla-security-standard/>) cybersecurity measures and policies. Cyber security statistics also includes a variety of other topics, but we have neither the time (nor the attention span) to cover all of them in one article. So, we'll limit it to several categories but will cover other areas in a future article.

So, what numbers have made our list of the 80 top cyber security statistics for 2019? As the saying goes around here: Let's hash it out.

Cyber security statistics: The cybersecurity industry overall and its economic outlook

While it's vital to stay abreast of the most recent cyber security attack statistics and information, it's also important to be aware of general statistics about cyber security as an industry overall, including its economic outlook. Depending on where you stand on the side of the cyber security market, the following statistics paint a positive or bleak outlook for your business concerning industry gender representation, profitability, or the mounting costs of protecting your business, customers, and data:

1 – $1.5 trillion cybercrime economy

The cybercrime economy has grown to enjoy *at least* $1.5 trillion in profits < https://www.thesslstore.com/blog/2018-cybercrime-statistics/> each year.

2 – 300 billion cybersecurity Market

The value of the cyber security market is anticipated to reach $300 billion by 2024, according to a 2019 press release < https://www.prnewswire.com/news-releases/cybersecurity-market-worth-over-300bn-by-2024-global-market-insights-inc--863930577.html> by Global Market Insights, Inc.

3 – $15 billion in cyber security funding

According to the 2019 President's Budget released by the White House, the U.S. government plans to spend on cybersecurity-related activities this year — a 4.1% increase ($583.4 million) over the 2018 budget. However, according to the budget document < https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf> , the caveat is that "Due to the sensitive nature of some activities, this amount does not represent the entire cyber budget."

4 – 9% increase in cyber security spending

Despite data breaches rising at inordinate rates each year, Juniper Research's Cybercrime & the Internet of Threats 2018 report <

https://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats-2018> anticipates cyber security spend will only increase by 9% on average per company, per annum.

5 – Small businesses invest <$500 per year in cyber security products

The average amount small businesses spend on consumer-grade cyber security products each year, according to Juniper Research's < https://www.juniperresearch.com/press/press-releases/cybersecurity-breaches-to-result-in-over-146> 2018 study. This constituted 13% of the overall cybersecurity market that year.

6 – Women anticipated to make up 20% of the cybersecurity workforce

Cybersecurity Ventures estimates that women will represent 20% of the global cybersecurity workforce by the end of the year, according to a company press release < https://www.prnewswire.com/news-releases/representation-of-women-in-the-cybersecurity-workforce-is-recalculated-to-20-percent-300821151.html> .

7 – 20% of CISOs anticipated to be women in 2019

Women are anticipated to hold 20% of Chief Information Security Officer (CISO) roles in the cybersecurity workforce by the end of the year, according to Forrester’s Cyber Predictions for 2019 < https://go.forrester.com/blogs/forrester-cyber-predictions-2019-european-take/> . This number is up from 13% in 2017.

8 – 49.6 day period between breach discovery and reporting dates

The number of days between when a data breach was discovered and reported was nearly 50 days in 2018, according to a report < https://pages.riskbasedsecurity.com/2018-ye-breachquickview-report> from security intelligence vendor Risk Based Security (RBS).

9 – >70% of cryptocurrency transactions for illegal activity

The percentage of all cryptocurrency transactions predicted to be used for illicit activity is anticipated to be 70% by 2021, according to the Cybersecurity Almanac 2019 < https://cybersecurityventures.com/cybersecurity-almanac-2019/> by Cybersecurity Ventures.

10 – Security breaches up >11%

The percentage by which security breaches have increased over the past year, according to the Ninth Annual Cost of Cybercrime < https://www.accenture.com/us-en/insights/security/cost-cybercrime-study> global study by Accenture.

Data Breaches
67% over 5 years

11 – Security breaches increased by 67%

Over the past five years, security breaches have increased by 67%, according to Accenture's global survey.

12 – SMBs are targeted 43% of the time

SCORE < https://www.prnewswire.com/news-releases/43-of-cyberattacks-target-small-businesses-300729384.html> reports that 43% of cyber attacks target small businesses.

13 – Ransomware attacks occur every 14 seconds

The frequency in which Cybersecurity Ventures predicts that a business will fall victim to a ransomware attack this year in its 2019 Official Annual Cybercrime Report <

https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> (ACR). The company also estimates that number will increase to every 11 seconds by 2021.

Cyber security statistics: The costs of cyber security attacks

The costs and damages that result from unaddressed cyber security vulnerabilities are, by no means, chump change. Cyber security attacks statistics should be an eye-opener for every company — particularly those that operate under the assumption (or with the hope) that a cyber attack will never happen to them. Anyone who thinks that their company — no matter how small or large — is not at risk because they lack cyber security vulnerabilities is fooling themselves. Simply put, as technologies evolve and cyber criminals become more advanced, it is a matter of *when*, not *if* < https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin> cyber security attacks will occur.

Here are some of the cyber security statistics relating to the costs of cybercrime and cyber security attacks:

14 – Cybercrime damages to reach $6 trillion annually

Cybercrime damages are anticipated to cost businesses and organizations $6 trillion annually by 2021, according to the 2019 ACR from Cybersecurity Ventures. This number, which is up from the company's 2015 estimate of $3 trillion in cybercrime damages annually, "represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined."

Ransomware
$20 Billion

15 – Ransomware damage estimated to reach $20 billion globally

The Cybersecurity Ventures annual crime report indicates that the same costs will reach **$11.5 billion** annually this year and $20 billion per year by 2021. Unsurprisingly, this type of year-over-year increase in anticipated damages makes ransomware the fastest-growing type of cybercrime in the past year.

16 – Cybercrime costs organizations $13 million per year

The average cost of cybercrime for an organization is estimated to be $13 million per year, according to Accenture’s global study.

17 – $1 cybercrime tools and kits

Cybercrime tools and kits can be purchased for as little as $1 on the Dark Web and online marketplaces, according to the Cybersecurity Almanac 2019 by Cybersecurity Ventures.

Cyber security statistics: Victim data and compromised records — by the numbers

When we’re talking about victims of cyber security attacks[, we’re referring to individuals, companies, and other organizations that are targeted or victimized in some way. The goal for cyber criminals is often to acquire information — personal information, names, addresses, financial and other account information, passwords, trade secrets, intellectual property, etc. — that can be used, traded, or sold on the Dark Web. They accomplish these goals through a variety of methods such as phishing and spear phishing emails < https://www.thesslstore.com/blog/hospital-employees-open-1-out-of-every-7-phishing-emails/> , URL hijacking, structured query language (SQL) injections, and man-in-the-middle (MitM) attacks < https://www.thesslstore.com/blog/man-in-the-middle-attack-2/> , as well as a litany of other methods.

In some cases, the goal is purely financial — they seek to manipulate and trick targeted employees into making large wire transfers to fraudulent accounts through business email compromise (BEC) < https://www.thesslstore.com/blog/macewan-university-phishing-scam-cautionary-tale/> and CEO fraud attack tactics. Why should the modern criminal go through the hassle of trying to rob a bank the old-fashioned way when they can get the employees at virtually any company to fork over thousands or even millions of dollars to them unwittingly?

Here is a glimpse of top cyber security threat statistics and cyber attack information relating to compromised victims and records:

18 – USA is No. 1

While this is something many Americans are usually proud to chant, in this case, it’s not necessarily a positive attribute. The United States holds first place in the ranks of the top countries that are targeted cyber security attacks, according to Norton Security < https://us.norton.com/internetsecurity-emerging-threats-

10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html> .

19 – 12 Breaches Results in +100 million exposed sensitive records

All it took was 12 data breaches to expose 100 million (or more) sensitive records in 2018, according to RBS's report. These 12 breaches accounted for nearly three-quarters of all records exposed that year.

60%
Of Americans have been exposed to fraud

20 – 60% of Americans exposed to fraud schemes

Sixty percent of Americans report they or an immediate family member have been victims of a scheme to defraud, according to research < https://www.aicpa.org/press/pressreleases/2018/nearly-half-of-americans-say-id-theft-likely-to-cause-themfinan.html> from The Harris Poll and the American Institute of CPAs (AICPA).

21 – 23% of Americans are cybercrime victims

Nearly one-quarter of surveyed Americans reported they or someone they know were victimized by cybercrime in 2018, according to Gallup's annual crime survey < https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx> .

22 – 31% of security professionals organizations victims of OT cyber attacks

Early one-third of surveyed security professionals say their organizations have experienced cyber attacks on operational technology (OT) infrastructure, according to Cisco's 2018 Security Capabilities Benchmark Study that was published in its 2018 Annual Cybersecurity Report < https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf> .

23 – Reported cybercrime victims only 10-12% of total

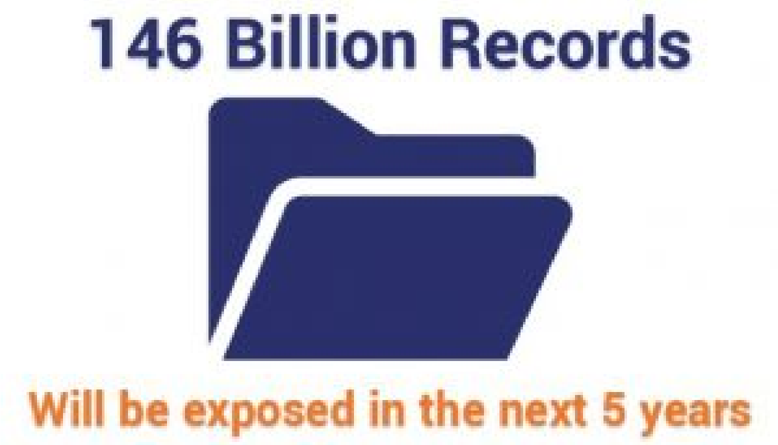
Donna Gregory, unit chief at the FBI's Internet Crime Complaint Center (IC3), estimated that only 10-12% of all U.S. cybercrime victims were reported in 2016, according to a New York Times article < https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html> .

24 – 76% of organizations and businesses were phishing targets

The number of organizations that were targeted by phishing attempts in 2017, according to Wombat Security's State of the Phish 2018 < https://info.wombatsecurity.com/hubfs/2018%20State%20of%20the%20Phish/Wombat-StateofPhish2018.pdf?submissionGuid=2ecea77c-aa0d-404a-b0f4-030732e60a3a> report.

25 – 33 billion records will be stolen

This is the number of records that Juniper Research's Cybercrime & the Internet of Threats 2018 report estimates cybercriminals will steal annually by 2023.



26 – 146 billion records will be exposed in data breaches

The number of records Juniper Research's 2018 report also estimates will be exposed by criminal data breaches between 2018 and 2023. The report specifies this number represents actual data breaches and not just reported data breaches.

27 – 88% of companies with >1 million folders don't limit access

According to a global study < https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf> of 130 organizations by Varonis, 88% of the companies with more than 1,000,000 folders lack appropriate access limitations — leaving 100,000 folders open to everyone (all employees). The report also indicates that 58% of the companies they surveyed have more than 100,000 folders accessible to all employees.

28 – 41% of companies allow all employees access to > 1,000 sensitive files.
Varonis's report indicates that 41% of the companies they surveyed have more than 1,000 sensitive files (those containing credit card information, health records, and personal information that is subject to regulatory compliance) open to all employees.

Cyber security statistics: Key cyber attack statistics by industry

Defining cyber security attacks can be difficult depending on how specific or generic you want to be in your definition. As such, trying to find the "top cyber attack methods" for each industry is virtually impossible because sources and researchers will define such attacks in different ways. For example, phishing emails can involve malware attacks, so researchers can choose to define them by either method.

With these considerations in mind, we've limited ourselves to highlighting just a few of the cyber security attack statistics relating to various industries:

29 – Ransomware attacks to increase 5X by 2021

The Cybersecurity Almanac 2019 from Cybersecurity Ventures estimates that ransomware attacks against healthcare organizations will increase by this amount between 2017 and 2021. This isn't all that surprising considering that healthcare ranks 15th out of 18 U.S. industries < https://www.thesslstore.com/blog/healthcare-industry-cybersecurity-2018/> with regard to cybersecurity and research shows that hospital employees open one of every seven phishing emails < https://www.thesslstore.com/blog/hospital-employees-open-1-out-of-every-7-phishing-emails/> .

30 – 48% of UK manufacturers are cybercrime targets

Nearly half of the surveyed manufacturers in the United Kingdom reported being victims of cybercrime or a cyber security incident at some point, according to a report < https://www.makeuk.org/insights/reports/2019/02/11/cyber-security-for-manufacturing> by Make UK and AIG that was carried out by the Royal United Services Institute (RUSI).

31 – 38.4% of mining industry users receive malicious emails

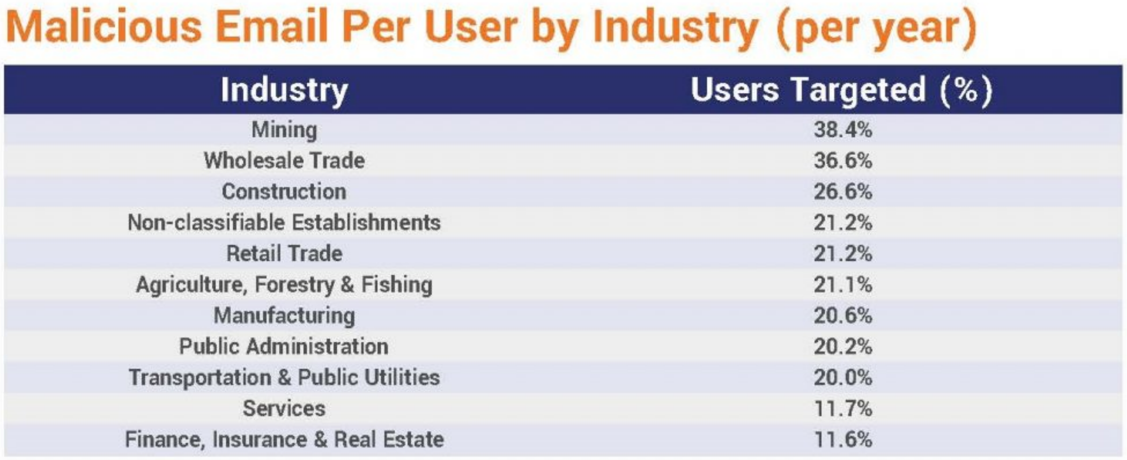
According to Symantec's Internet Security Threat Report (ISTR) 2019 < https://www.symantec.com/security-center/threat-report> report, 38.4% of users in the mining industry were targeted with malicious emails.

32 – 1 in 302 emails targeting public administration users are malicious

Email users working in the public administration sector receive one malicious email for every 302 emails they receive, according to Symantec's ISTR 2019 report.

33 – >20 ATM malware families now exist

According to Kaspersky Lab, there are now more than 20 ATM malware families < https://securelist.com/ksb-cyberthreats-to-financial-institutions-2019-overview-and-predictions/88944/> that pose threats to the banking and finance industry.



Malicious Email Per User by Industry (per year)

Industry	Users Targeted (%)
Mining	38.4%
Wholesale Trade	36.6%
Construction	26.6%
Non-classifiable Establishments	21.2%
Retail Trade	21.2%
Agriculture, Forestry & Fishing	21.1%
Manufacturing	20.6%
Public Administration	20.2%
Transportation & Public Utilities	20.0%
Services	11.7%
Finance, Insurance & Real Estate	11.6%

Cyber security statistics: Top data breaches of 2018 and 2019 (so far)

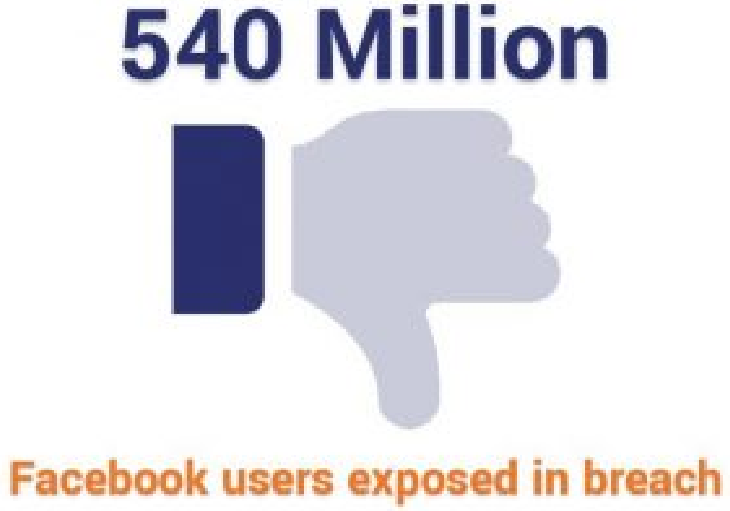
Cyber security research and reports from the past several years indicate that cyber attacks are rapidly increasing and the number of new attacks will surpass those of previous years. Here are some cyber security attacks that were reported in 2018 and 2019:

34 – Personal info of 1.5 billion Indian citizens exposed in Aadhaar data breach

The personal information of 1.5 billion Indian citizens (photographs, national ID numbers, phone numbers, addresses, postal codes, and email addresses) was exposed in a massive data breach < https://www.csoonline.com/article/3341317/data-breaches-exposed-5-billion-records-in-2018.html> of the nation's ID database that was discovered in March 2018.

35 – 1.16 billion email addresses and passwords exposed

The number of "unique combinations of email addresses and passwords” that was discovered in 2019 in a massive breach called “Collection 1.” This load of information was discovered by an IT security researcher and is thought to be the largest breach in history to date, according to an article < http://fortune.com/2019/01/17/collection-1-data-breach/> by Fortune.



36 – 540 million Facebook users exposed in breach announced in 2019

More than half a billion records about Facebook users were publicly exposed in two app datasets that were digitally stored in two Amazon Simple Storage Service (S3) storage buckets, according to a 2019 announcement by UpGuard < https://www.upguard.com/breaches/facebook-user-data-leak> .

37 – Marriott breach exposes 500 million user accounts

This statistic reflects the number of user accounts that were exposed in a data breach of Marriott's Starwood guest database < https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/> , which was disclosed in 2018.

38 – 340 million contacts exposed in Exactis data breach

The personal information of 340 million U.S. consumers and business contacts was exposed on a publicly accessible server by Exactis, a marketing and data aggregation firm, according to a report < https://www.cnet.com/news/exactis-340-million-people-may-have-been-exposed-in-bigger-breach-than-equifax/> by CNET.

39 – 200 million user accounts exposed via Fortnite cyber security vulnerability

The number of Fortnite user accounts were exposed when hackers took advantage of an old, unsecured website page < https://www.cbsnews.com/news/fortnite-security-flaw-exposed-millions-of-users-to-being-hacked/> to send phishing emails. The flaw was reported in Check Point Research’s January 2019 announcement < https://research.checkpoint.com/hacking-fortnite/> .

40 – 30 million users exposed in 2018 Facebook data breach

In 2018, 30 million Facebook users were affected by another data breach, according to Consumer Reports < https://www.consumerreports.org/digital-security/facebook-data-breach-exposed-personal-data-of-millions-of-users/> . Nearly half (14 million) of those users’ sensitive information was accessed, and the names and contact information of another 15 million were also exposed.

Cyber security statistics: Most common types of cyber attacks

Cyber security attacks are some of the fastest-growing crimes in the world — especially for businesses and organizations in the United States. (Juniper Research estimates that the U.S. companies and organizations will be the targets of more than 50% of all cyber attacks by

2023.) As such, there are a lot of statistics in this area that we can cover, including a breakdown of some of the top cyber security threats and a list of some of the most common types of cyber attacks.

In terms of cyber security threats statistics, we’ve put together a list which includes DDoS attack statistics, malware attack statistics, man-in-the-middle attack statistics, phishing-related statistics, and web application attacks and vulnerabilities:

DoS and DDoS attack statistics

Although the methods and scale of each attack differ, the ultimate goal of denial of service (DoS) and distributed denial of service (DDoS) attacks is the same: The aim is to flood a resource or targeted system to deny access to those who need it.

Internet of Things (IoT) devices are frequently compromised and added to botnets, then used to launch ongoing distributed denial of service malware and brute-force attacks that use common usernames and passwords. As the IoT market continues to grow and more devices are being used across virtually all industries, we anticipate the year’s cyber security statistics will continue to reflect increasing cyber attacks and exploits of this technology in 2019.

41 – 20.4 billion

The anticipated number of Internet of Things (IoT) devices that will exist by 2020, according to a press release < https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016> from Gartner, Inc.

42 – Routers account for 75% of infected devices in IoT attacks

Routers accounted for 75% of IoT attacks in 2018, and connected cameras accounted for 15% of them.

43 – The largest DDoS attack on record: 1.7 TBPS

The largest DDoS attack on record, according to NETSCOUT Threat Intelligence Report < https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf> from the second half of 2018, was a 1.7 terabytes per second (TBPS) reflection/amplification attack < https://www.netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era> against a U.S.-based service provider. To provide you with perspective, Netflix recommends five megabits per second for streaming high definition (HD) quality shows and 25 megabits per second for streaming ultra HD quality shows. Eight megabits is equal to one megabyte per second, and one million megabytes is equal to one terabyte. This means that the victim was targeted with an attack using the demand equivalent of streaming 200,000 HD TV shows, or 40,000 ultra HD TV shows, simultaneously.

44 – DoS or DDoS attack could cost enterprises $2 million

According to the Annual Cyber Security Report 2019 < https://www.bulletproof.co.uk/industry-reports/Bulletproof%20-%20Annual%20Cyber%20Security%20Report%202019.pdf> report from Bulletproof, a DoS or DDoS attack could cost an enterprise company more than $2 million or up to $120,000 for a small company.

5 Minutes
Amount of time it takes for an IoT device
to be attacked after going online

45 – IoT devices typically attacked within 5 minutes

Five minutes is the amount of time it takes for an IoT device to be attacked once plugged into the Internet, according to a report from NETSCOUT.

46 – China accounted for more than 50% of DDoS attacks in Q4 2018

The percentage of distributed denial of service attacks that originated in China in Q4 2018 fell to 50.43% from 77.67%, according to Kaspersky's DDoS Q4 Report < https://securelist.com/ddos-attacks-in-q4-2018/89565/> . The United States came in second with nearly **25%** and Australia in third with **4.5%**.

47 – $20 price tag for DDoS attacks

The low cost per target to purchase a DDoS attack ranging from 290 to 300 gigabits per second, according to an ARS Technica article < https://arstechnica.com/information-technology/2018/02/for-sale-ddoses-guaranteed-to-take-down-gaming-servers-just-20/> .

Malware attack statistics

According to an article by Security Magazine < https://www.securitymagazine.com/articles/89362-in-50-emails-contain-malicious-content> , one in 50 emails contain some form of malicious content. As we turn our attention to malware attacks, it is an area of attack that shows no sign of slowing in 2019. Digital Trends < https://www.digitaltrends.com/computing/1-percent-of-malicious-emails-contain-malware/> estimates that 10% of all malicious emails contain malware such as ransomware, spyware, adware, or trojans. Here are some additional cyber security statistics to help increase your understanding of this growing issue:[

48 – 1,000% increase in malicious PowerShell scripts

The use of malicious PowerShell scripts increased 1,000%

in 2018, according to Symantec's ISTR 2019 report

49 – Email responsible for spreading 92% of all malware

CSO Online < https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html> estimates that email is the primary method of malware delivery

Microsoft Office
Microsoft office files accounted for 48%
of all malicious email attachments in 2018

50 – Office files constitute 48% of malicious email attachments

Forty-eight percent of malicious email attachments were Microsoft iOffice files in 2018, according to Symantec's ISTR 2019 report.".Doc" or ".dot" files represented **37%** of malicious email attachments.

51 – Mobile ransomware jumped 33% last year

In 2018, the prevalence of mobile ransomware increased by 33%, according to Symantec’s ISTR 2019 report.

52 – Enterprise ransomware increased 12% in 2018

Last year, enterprise ransomware increased 12%, according to Symantec’s ISTR 2019 report.

53 – Scripts represent 47.5% of malicious email attachments

Nearly 48% of malicious email attachments are scripts, according to Symantec’s ISTR 2019 report.

Man-in-the-middle attack statistics

Man-in-the-middle attacks are, essentially, the modern form of old-fashioned eavesdropping. However, it’s not that simple — MitM attacks also include the use of content injection or alteration as well as other tactics. Here are some cyber security statistics relating to MitM attacks and methods:

Are vulnerable to Man-in-the-Middle attacks

54 – 95% of HTTPS servers vulnerable to MitM

According to Netcraft, MitM attacks < https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html> were thought to pose a threat to 95% of HTTPS servers in 2016.

55 – MitM attacks were involved in 35% of exploitations

More than one-third of exploitation of inadvertent weaknesses involved MitM attacks, according to IBM's X-Force Threat Intelligence Index 2018 < https://www.ibm.com/downloads/cas/MKJOL3DG> .

56 – 10% of companies implement HSTS

Only 10% of companies have implemented HTTP Strict Transport Security (HSTS) for websites, according to research < https://w3techs.com/technologies/details/ce-hsts/all/all> from W3Techs.

Phishing statistics

By and large, phishing leads the pack when it comes to the most common types of cyber attacks against businesses. Cofense, formerly PhishMe, reports < https://cofense.com/enterprise-phishing-susceptibility-report/> that 91% of cyber attacks start with a spear-phishing email. Here are some additional phishing statistics that you should know:[

57 – SaaS-mimicking phishing attacks increased 237%

Phishing attacks mimicking Software-as-a-Service platforms increased 237% in 2017, according to Phish Labs's 2018 Phishing Trends & Intelligence Report < https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf> .

58 – BEC costs U.S. companies $12.5 billion

The Federal Bureau of Investigation (FBI) reported < https://www.ic3.gov/media/2018/180712.aspx> $12.5

billion in losses to companies between October 2013 and May 2018 due to business email compromise (BEC).

59 – U.S. target of 86% phishing attacks

Phish Labs reports that 86% of phishing attacks targeted U.S. victims.

60 – 83% of infosec professionals experienced phishing attacks in 2018

Eighty-three percent of global information security respondents experienced phishing attacks in 2018, according to ProofPoint’s State of the Phish 2019 Report < https://info.wombatsecurity.com/hubfs/Wombat_Proofp oint_2019%20State%20of%20the%20Phish%20Report_Final.pdf> .

61 – Phishing, pretexting represent 98 and 93% of social incidents and breaches

Verizon's 2018 Data Breach Incident Report < https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf> states that "phishing and pretexting represent 98% of social incidents and 93% of breaches."

Web application attacks and vulnerabilities

Web applications — everything from calculators and Google docs to webmail platforms and dynamic websites — are vulnerable to a variety of attack methods such as SQL injections, formjacking, and brute force attacks. According to a report < https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/> by Imperva:

> *“The overall number of vulnerabilities in 2018 (17,308 increased by 23% compared to 2017 (14,082) and by 162% compared to 2016 (6,615)… more than half of web application vulnerabilities have a public exploit available to hackers. In addition, more than a third (38%) of web application vulnerabilities don’t have an available solution, such as a software upgrade workaround or software patch.”*

Web application vulnerabilities create opportunities for hackers to launch devastating attacks. Hackers launch many types of web application cyber attacks — TrustWave < https://www2.trustwave.com/rs/815-RFM-693/images/Trustwave_2018-GSR_20180329_Interactive.pdf> reports the two most common attack method as cross-site scripting (XSS), which constituted about 40% of web attack attempts, and SQL injections (24%).

The following is a list of key cyber security statistics relating to web application attacks and vulnerabilities:

62 – 46% of websites have high cyber security vulnerabilities

Acunetix's Web Application Vulnerability Report 2019 < https://cdn2.hubspot.net/hubfs/4595665/Acunetix_web_application_vulnerability_report_2019.pdf> reports that websites have **46%** high and **87%** medium security vulnerabilities.

63 – SQL injection and cross-site scripting saw a 38% increase

"Application-layer attacks such as SQL injection or cross-site scripting" increased 38%, according to Akamai's

Summer 2018 State of the Internet/Security: Web Attack < https://www.akamai.com/us/en/about/news/press/2018-press/akamai-releases-summer-2018-state-of-the-internet-security-report.jsp> report.

64 – Formjacking compromised 4,818 websites monthly in 2018

The average number of websites compromised by formjacking code each month in 2018 was 4,818, according to Symantec’s ISTR 2019 report.

65 – 2% of web applications susceptible to RCE

Acunetix’s Web Application Vulnerability Report 2019 indicates that 2% of its sampled web application targets were vulnerable to remote code execution, which allows a malicious user to execute virtually any code within a web application.

66 – Two TLS vulnerabilities decrease to 0% and 3%

As TLS version 1.3 < https://www.thesslstore.com/blog/tls-1-3-approved/> becomes more prevalent, old SSL and TLS vulnerabilities such as Heartbleed and POODLE (affecting TLS versions up to 1.2 < https://www.thesslstore.com/blog/zombie-poodle-and-goldendoodle-two-new-exploits-found-for-tls-1-2/>) have decreased across the internet or become virtually nonexistent, dropping to 0% and 3% of websites respectively, according to Acunetix's Web Application Vulnerability Report 2019.

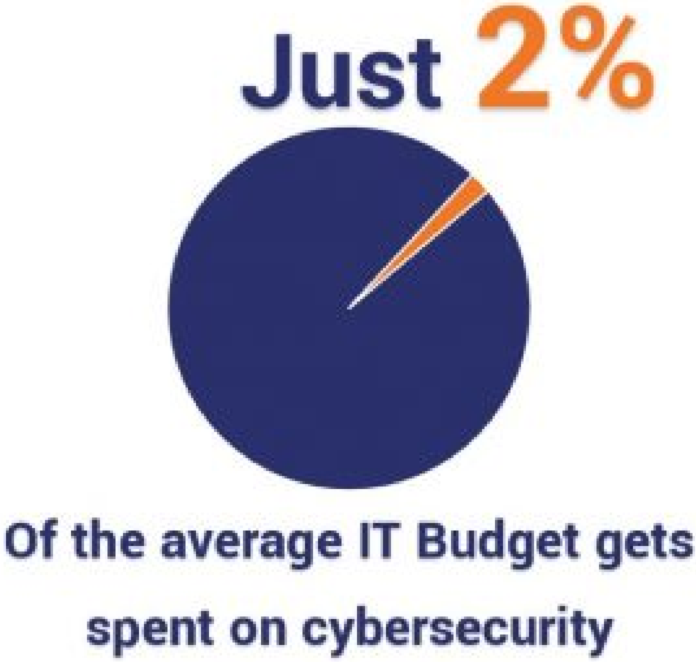
67 – 75% of LAN penetration due to web application weaknesses

Three-quarters of network penetration vectors resulted from poor web application security protections, according to a 2019 report on vulnerabilities in corporate information systems < https://www.ptsecurity.com/ww-en/analytics/corp-vulnerabilities-2019/> by Positive Technologies.

Cyber security statistics: Compliance with cyber security industry best practices

Ideally, every company, government, and organization should follow industry best practices to ensure their IT infrastructure, data, and customer information are secure. However, we've long since come to realize that expectations and reality are often two very different things. Recent research indicates that most companies lack adequate data protections and have not implemented cyber security best practices. This leaves them vulnerable to data loss, financial costs, and reputational harm.

Here is our list of some of the most enlightening recent cyber security statistics we could find concerning compliance issues and industry best practices:



68 – Only 2% of IT budget is used for security

ZDNet reports < https://www.zdnet.com/article/cybersecurity-is-broken-heres-how-we-start-to-fix-it/> that only 2% of companies' IT expenditure last year was used on security measures.

69 – 70% of employees don't understand cybersecurity

The percentage of U.S. employees who lack a basic understanding <

https://www.thesslstore.com/blog/report-70-us-employees-lack-strong-knowledge-privacy-security-best-practices/> of cybersecurity best practices is estimated to be 70%.

70 – 32% of U.S. companies failed to properly implement SSL/TLS

High-Tech Bridge < https://www.htbridge.com/blog/FT500-application-security.html#3.2> reports that 32% of U.S. companies (16% of European companies) received failing grades for their implementations of SSL/TLS encryption, according to High-Tech Bridge's report < https://www.htbridge.com/blog/FT500-application-security.html#3.2> .

71 – 52.5% companies compliant with PCI DSS requirements

More than 50% of companies were estimated to be fully compliant with interim PCI DSS (Payment Card Industry Data Security Standard) requirements in 2017, according to Verizon's 2018 Payment Security Report < https://enterprise.verizon.com/resources/reports/2018_payment_security_report_en_xg.pdf> .

72 – 30% of the world’s top websites unsecure

Whynohttps.com < https://whynohttps.com/> estimates that 30% of the world’s top 560 websites are not secure. These sites include ESPN.com, BBC.com, Wikia.com, MyShopify.com, Chegg.com &NBA.com.

73 – 93% of companies report implementing password rules

Of the 93% of companies that report having password rules, fewer than 25% require mandatory password changes and 53% require quarterly changes, according to data cited by TechRepublic < https://www.techrepublic.com/article/93-of-companies-have-password-rules-but-it-may-not-protect-them-from-data-breaches/> in a OneLogin survey.

74 – Outdated and unpatched software constitutes 22% of security issues

According to BulletProof’s 2019 report, 22% of the high and critical-risk issues reported consisted of missing patches, out-of-date or no longer supported software.

75 – 68% of business don’t have cyber security insurance

More than two-thirds of businesses neglect to purchase cyber liability or data-breach insurance < https://www.thesslstore.com/blog/cyber-insurance/> coverage, according to a Cisco’s 2018 Cyber Security and Insurance < https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/cybersecurity-solutions/cyber-security-insurance-aag.pdf> paper.

76 – 68% don’t have a disaster recovery plan in place

More than two-thirds of small business owners lack a disaster recovery (DR) plan, according to a study < https://blog.nationwide.com/news/disaster-recovery-plan-study-results/> by Nationwide. The company also reports that **71%** of small business owners do not purchase business interruption insurance.

77 – 45% of companies have a uniform encryption strategy or plan

Fewer than half of surveyed companies report having an encryption plan or strategy that is applied consistently across their enterprises, according to the Ponemon Institute's 2019 Global Encryption Trends Study < https://go.ncipher.com/rs/104-QOX-775/images/2019-Ponemon-Global-Encryption-Trends-Study-ar.pdf> for nCipher Security.

78 – 73% of companies have minimum cyber security requirements for vendors

The percentage of organizations that now require third-party vendors to meet minimum cyber security requirements, according to a BDO USA's 2018 cyber governance survey < https://www.bdo.com/insights/assurance/corporate-governance/2018-bdo-cyber-governance-survey-board-perspecti> .

79 – 95% of employees/end users receive phishing training

We're happy to share that 95% of survey respondents report training employees/end users to identify and avoid phishing attacks, according to ProofPoint's State of the Phish 2019 Report

80 – 60% of organizations use cloud technology for sensitive or confidential data

Almost two-thirds of respondents for the Ponemon Institute/nCipher Security survey say their organizations transfer confidential or sensitive information to the cloud regardless of whether the data is encrypted or made unreadable.

While there are many other cyber security statistics out there relating to the industry, attacks, and vulnerabilities, we can’t cover all of them in one single post. However, many aspects of these statistics will be covered in future Hashed Out blog posts. Be sure to keep an eye out for our upcoming blog post on the topic of the 2019 cybercrime statistics in particular.

Final thoughts

While cybercriminals represent a significant threat to companies, organizations, and governments alike, it’s easy to see that they are not the only threats or even the biggest ones. In most cases, the critical threats to organizations are their own lack of adequate defenses < https://www.thesslstore.com/blog/71-of-organizations-dont-know-how-many-certificates-keys-they-have/> and employees who are ignorant of cyber threats < https://www.thesslstore.com/blog/report-biggest-cyber-security-threat-employees/> . Organizations can reduce their risks of cyber attacks by following industry best practices and implementing key defense measures such as employee training and the use of encryption < https://www.thesslstore.com/blog/gdpr-encryption-best-practices-wp29/> .

What are some of the important and recent cyber security statistics that you’ve discovered? As always, we invite you to leave any comments or questions in the comments section below.